AUTHENTICATION FOR ONLINE TRANSACTIONS USING TOKENS VIA MOBILE PHONES

P.M.D.ALI KHAN, T.K.LAKSHMI, P.J. SARACHANDRIKA
Asst.professor, C.S.E, S.V.College of Engineering, TPT
Asst.Professor I.T, S.V.College of Engineering, TPT
Asst.professor, C.S.E, S.V. College of Engineering, TPT
pathan.md@gmail.com, rohiniraman103@yahoo.com, sarachandrika@gmail.com

ABSTRACT
As online transactions require new authentication methods, banks are trying to introduce new approaches in order to prevent attacks being successful and to increase security. Besides usual username/password (or similar) approaches, additional tokens are applied for authentication in order to make online-banking more secure. Online banking authentication plays an important role in the field of online banking security. In past years, a number of methods, including password token, short message password, and USB token, have been developed for online banking authentication. The proposed method guarantees that authenticating to services. We provide attack analysis to illustrate the strength of the protocol. The generated digital certificate is valid for only a short user defined period of time and is generated by factors that are unique to both, the user and the mobile device itself. Additionally, an SMS-based mechanism is implemented as both a backup mechanism for retrieving the password and as a possible mean of synchronization.

Keywords: Online Banking; Authentication Protocol; Mobile Phone; Digital Certificate

1. INTRODUCTION
Online banking history can be traced back to the mid of 1990s, an era when Internet usage is not popular. With the rapid development on computing technologies and cyber networks, by the end of 2005, about 63 million of American adults use online banking [1]. Nowadays, online banking has surpassed bank branches and ATMs and becomes the most favorite banking method of Americans [2]. Nevertheless, technology has long been considered as a double-edged sword: when people are enjoying the convenience brought by online banking, their accounts information is also subject to be stolen or tampered by Internet criminals. Thus, client authentication in their online banking process has become a critical security concern for financial institutions.

Online banking authentication typically asks for username and password. However, there are few security mechanisms being applied to protect username, since it is typed in plaintext at login process and it may not be encrypted during transmission. On the other hand, securely managing passwords is quite tricky for the majority of people. If a password is short or has some clues making it easy to remember, it is weak against potential attacks. One can certainly make a strong password forget it or has to write it down somewhere to remind himself later. Furthermore, an emerging trend of phishing attacks [3] leads to an increasing number of phishing websites which dupe victims typing out their passwords by their hands. Hence the less the password security relies on human meditation, the more it is secure.

Correspondingly, various solutions focusing on solving the security issues of online banking password authentication have been developed. A Password-Generating Token (PGT) [4] is a portable device that can generate a certain digit number every 60 seconds. A good example of the implementation of PGT is RSA’s SecureID [5] which requires making use of it to login the online banking system together with a client’s original password. One-Time Password (OTP) is, of course, another solution. After a client provides her username and original password to the bank via Internet, a one-time password is sent to her mobile phone within a Short Message Service (SMS) message [6]. This client then retrieves the OTP and uses it for a further login. Biometrics is also a security concern of online banking authentication [4], where a user needs to authenticate himself by conducting iris or fingerprint scans or voice confirmations.

Public-key Infrastructure (PKI) has been applied to online authentication. Hypertext Transfer Protocol Secure (HTTPS) is prevalently adopted even not only for online banking authentication but also for online shopping and email system authentications. With the implementation of HTTPS, a client is able to be authenticated by providing her digital certificate (DC) to the bank. A former approach includes integrating a client’s DC into a USB flash drive, which becomes a USB Token [4]. Our solution falls into this category making a client’s mobile phone to store her certificate instead of the flash drive.

The rest of paper is outlined as follows. In section II, we describe the related work. In section III, we introduce our approach. We conduct security and attack analysis in section IV and provide a conclusion in section V.

2. RELATED WORK
A. Online Authentication
Authentication is a security measure designed for verifying an individual’s identity through validating his
credentials usually before the individual is given the access to certain information or systems. Loosely speaking, online authentication is to verify identities through cyber networks. While under a closer scrutiny, online authentication has its unique three security issues worthy to be considered: First, how can we make sure the website that an individual wants to contact with is the accurate site? Second, how can we safeguard an individual’s credentials during their transmission? Third, how can we judge that these credentials are really from the individual whom the sender claims to be?

HTTPS is now being widely used for online banking authentication. At first, bank proves its identity by sending its DC, issued by a certificate authority (CA) like VeriSign, to one client. Information in the certificate includes the issuer’s name, certification validation period, version number, serial number, subject, etc [7]. This client then validates the certificate and provides his credential to the bank. At last, the bank verifies the client’s identity and starts the communication under a symmetric encryption.

The first two security issues have been solved quite well with the implementation of SSL: A digital certificate has a CA’s digital signature which makes it impossible to forge and every client’s credential is encrypted with bank’s public-key that only the bank is able to decrypt it. Multi-factor authentication [4] is suggested by Federal Financial Institutions Examination Council (FFIEC) in response to the third security issue as well as today’s risky Internet environment. However, people often lose, break, or forget their token devices as if they cannot securely manage their passwords. Besides, mobile phone OTP is subject to leakage since SMS message is transmitted in plaintext which leaves attackers to eavesdrop. A client’s digital certificate resembles a bank’s DC. Information including name of the client, address, date of birth, and telephone number is signed by a CA and stored in a USB flash drive. By the time a client wants to login her account, this USB Token needs to be plugged in order to provide her certificate. Moreover, this solution offers a client digital signature on each transaction by encrypting it using the client’s private key as the transaction is being confirmed from the perspective of the client.

B. Trusted Platform Module and USB Token Disadvantages

Given the popularity of using asymmetric encryption algorithms to protect authentication security, how to securely store private keys has become an issue. To answer the question, USB Token has a particular file system to hold the private key which makes the key useable but unreadable as well as unwritable. The system denies any command from anyone trying to read and write the private key.

Trusted Platform Module (TPM) [14] is a microchip that is able to securely store authentication elements such as encryption keys and digital certificates. USB Token scheme has its indisputable advantages as an online authentication solution. But it also exposes a couple of defects. It is awkward to use because one client has to carry an extra USB flash drive whenever she wants to do online banking. If the Token is lost, it may not be a big issue but it does impede the client’s online banking capability for a while. A more serious flaw is that the scheme cannot prevent fake transactions from being signed. Suppose the client’s computer has been taken over by a hacker, it is feasible for the hacker to modify a transaction whereas it still appears to be the original one to the client. Without realizing what has been changed, a modified transaction will be confirmed by the client anyway.

C. Mobile Phone Online Banking Authentication

Motivated by the previous work, we have developed our solution for online banking authentication by using mobile phone to store and provide client digital certificate as well as conduct transaction confirmations in order to prevent fake transactions from being signed.

3. OUR APPROACH

In this section, we will describe the details of authentication protocol and transaction confirmation protocol respectively. Before the protocol starts, we assume that client’s mobile phone has TPM Embedded and connected with a personal computer via a USB cable or Bluetooth.

A. Mobile Phone Online Authentication Protocol Steps

The related notations and protocol steps are described below.

- C -- Client
- M -- Mobile Phone
- P -- Client’s PC
- S -- Bank’s Server
- PIN -- Personal Identification Number
- Rk -- Random generated number by P
- Rs -- Random generated number by S
- H() -- Secure Hash Function
- PKc -- Client’s Public Key
- PVc -- Client’s Private Key
- PKb -- Bank’s Public Key
PV_B -- Bank’s Private Key

\{data\}_K -- data is encrypted by Key (K)

1. A client starts a HTTPS connection with the bank by visiting the bank’s login web page. The detail of HTTPS connection is described as follows:
   (1) P says ‘Hello’ to S: As the beginning step, cipher configuration that documents the available cipher algorithms on P as well as a random generated number R_C are sent to S.
   (2) S says ‘Hello’ to P: S reviews the configuration and sends back its cipher choices together with the bank’s certificate, a R_S, and a client digital certificate request.
2. Based upon a successful verification of bank’s certificate, M displays a message prompting C to input the PIN, which is used to prove the current holder of M is the real C.
3. Types the PIN using M’s keyboard.
4. C’s certificate combined with PK_C, a C’s signature, and a pre-master piece, which is encrypted by PK_B, are sent to S after the right PIN is provided. C’s signature is in the pattern: \{H(R_C,R_S)\}_PV_C.
5. S first verifies C’s certificate, then validates its signature through decrypting it using PK_C and comparing the hash result. At last, S calculates a symmetric key, SK, for further usage. The SK is generated based on the knowledge of R_C, R_S, and the pre-master piece.
6. P generates a same SK and the further communication between P and S will be encrypted by SK. At this point, authentication process is successfully finished.

A client digital certificate can be acquired at bank by the time a client opens her account or downloads it from bank’s website afterwards. And a client’s public-private key pair is able to be generated within her mobile phone by TPM. The verification of bank’s certificate at step 2 is actually carried out by P’s browser. If the verification is failed, the authentication process will be terminated immediately.

B. Transaction Confirmation Functionality

It is controversial that today’s PC has become an untrusted device [16]. However, with ubiquitous malware such as Trojan Horses and Backdoors, a computer connected to the Internet is apt to be manipulated by hackers or even script kiddies.

Both the appearance and functionality of a mobile phone have been changed a lot from its bulky and powerless predecessors within a past few years. Today, mobile phone resembles a mini personal computer that commonly possesses a keyboard and an operating system. Unfortunately security menace like malware, which used to solely exist on PCs, has been ported on mobile phones.

Cabir [17], a Bluetooth worm, takes advantage of Bluetooth channels on the mobile phone running Symbian system to spread itself onto others. For its propagation [18], a target device will display a message that asks its user for a confirmation of receiving a message via Bluetooth. If the user allows his phone to receive the message, the worm will be installed on it. After this, Cabir is going to force its host searching for other available targets to continue propagating. Besides Cabir, a mobile phone Trojan named Skulls [19] infects victim device by replacing its program icons with the images of skulls and crossbones as well as disables many applications. The only way to remove the Trojan is to use third party file managers [18].

Despite its dreadful spread capability, Cabir has quite weak affections on its host: it just depletes the battery or hinders the use of Bluetooth [18]. Fortunately, the attack of Skulls is easy to be protected since there are warnings showing to users prior to the real infection [19]. Moreover, based on the fact that there is not any devastating event happened due to mobile phone malware till now, we believe that mobile phones are still in a relative better security environment than PC’s peripherals. Therefore, using mobile phone as a media to store and process authentication components is reasonable.

C. Attack Analysis of Our Protocol

Attacks that can be applied to the protocol are thoroughly described and analyzed in this section. To make the description clearly, we sort the attacks into two categories: Remote Attack and Local Attack.

1) Remote Attack: Remote attack indicates an attacker, who does not have possibility to get access to the client’s
mobile phone, attacks remotely through phishing, pharming, session hijacking, and remote desktop attacks [16].

- Phishing: Phishing attack usually targets on victim’s username and password. Since users of our authentication protocol do not need to provide their passwords, this type of attack should not be accepted. Even in a very unlikely event that the attacker intends to collect the digital certificate of client. Before he can receive a client’s DC, he must provide a fake one to deceive the client which is unfeasible.
- Session hijacking: Skillfully conducting man-in-the-middle attack between a client and the bank server may direct the communication, which intends to be received by the client, going to the attacker. However, without the client’s mobile phone, the attacker should not be able to confirm any transaction.

Local Attack: Compared with remote attack, local attack happens when the attacker has access to clients’ mobile phones. However, situations will be different depending upon whether the attacker is a stranger or an acquaintance to the clients.

Attacker is a stranger. In this situation, the first challenge for the attacker is to access the phones. Stealing a mobile phone without being noticed by its owner seems hard to do, but it may be a little bit easier for the attacker to conduct a pocket pick when both of them are crowded by many other people, such as on a subway or in an elevator. Usually a third challenge coming together with guessing the PIN is a lock out session. It means if the attacker cannot type in the right PIN within the limited input times, usually three, the client’s DC will be locked which requires the client to unlock it under help of a banking attendant. Besides the client can call the banks help desk to disable his digital certificate after lost. Obviously, a successful attack needs to overcome these four challenges which make such an attack nearly impossible.

CONCLUSIONS
This paper introduces the concept of an online banking authentication protocol that involves the use of mobile phones to securely store clients’ digital certificates. It also provides Transaction Confirmation Functionality to prevent fake transactions from being signed by the innocent clients. We describe mobile phone security and potential attacks towards the protocol. By categorizing all of the attacks into two collections, we are able to clearly notice that the protocol is immunized to all of the remote attacks. For the local ones, an attacker still has a significant low probability to achieve a successful attack due to the inherent and integrated challenges of the protocol. However, the probability may be increased under the situation where the attacker is an acquaintance of the target client. In this case, it is worthwhile to lower the risk as our future work

REFERENCES
http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary